UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,404	11/03/2003	Benjamin Wilken	12221-020001	6346

26161 7590 04/02/2008

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
BESROUR, SAOUSSEN	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
04/02/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/701,404	WILKEN ET AL.	
	Examiner	Art Unit	
	SAOUSSEN BESROUR	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-17 and 19-36* is/are rejected.

7)☒ Claim(s) *5,13 and 18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/19/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to amendment filed 12/19/2007. Claims 1, 4, 5, 11, 12, 14, 17, 18, 24, 27, 28, 31 and 32, were amended. Claims 36 are pending.

Response to Arguments

2. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

Allowable Subject Matter

3. **Claims 5, 13 and 18** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1-4, 6-17 and 19-36** are rejected under 35 U.S.C. 102(e) as being anticipated by Pruthi (20040015582).

As per **claim 1**, Pruthi discloses: adding host-pair connection records to a connection table when a host accesses another host (0036, 0039, 0187); at the end of a firstupdate period, accessing the connection table to determine new host pairs (0039); determining the number of new host pairs added to the table over the first update period (0187); and if a host has made more than a first threshold number "C 1" host pairs, a historical number of host pairs in the profile is smaller than the threshold number by a first factor value "C2", then indicating to a console that the new host is a scanner (0187, 0204-0205).

As per **claim 8, 20 and 33**, Pruthi discloses: retrieving from a connection table logged values of protocols and ports used in host pair connections records in the table (0046); determining if the number of ports used in the historical profile is considerably smaller by a factor "C 1" than a current number of ports being scanned by a host and the current number is greater than a lower-bound threshold "C2", to record the anomaly (0187, 0204-0205); and reporting a port scan to a console (0187, 0204-02058).

As per **claim 14, 24 and 28**, Pruthi discloses add host-pair connection records to a connection table when a host accesses another host, at the end Of a first update period, accessing the connection table to determine new host pairs (0036, 0039, 0187); determine the number of new host pairs added to the table over the update period (0036, 0039, 0187); and if a host has made more than a first threshold number "CI" host pairs, and a historical number of host pairs in the profile is smaller than the threshold number by a first factor value "C2", then indicate to a console that the new host is a scanner (0187, 0204-0205).

As per **claim 2, 15, 25 and 29**, rejected as applied to claim 1, 14, 24 and 28. Pruthi discloses wherein "CI" and "C2" are adjustable thresholds (0187-0188).

As per **claim 3, 16, 26 and 30**, rejected as applied to claim 2, 14, 24 and 28. Pruthi discloses wherein the connection table is a current time-slice connection table and host pair records are added to the current time slice connection table (0187-0188).

As per **claim 4, 17, 27 and 31**, rejected as applied to claim 3, 16, 24 and 28. Pruthi discloses aggregating records from the current time-slice table into a long update period table, the second update period table having a period that is greater in duration than the first update period (0041); and checking for ping scans at the end of a long update period (Column 7, Lines 30-45); and indicating hosts which produced more than "C3" new host pairs over the second update period (0187-0190).

As per **claim 6, 19**, rejected as applied to claim 1, 14. Pruthi discloses maintaining Address Resolution Protocol (ARP) packet statistics in the connection table and for sparse subnets tracking the number of generated ARP requests that do not receive responses to detect scans on sparse sub-networks (0035, 0042, 0109, 0202).

As per **claim 7**, rejected as applied to claim 1. Pruthi discloses: the scanning attack is a ping scanning attack (0187).

As per **claim 9, 21 and 34**, rejected as applied to claim 8, 20 and 33. Pruthi discloses assigning a severity level to the port scan and reporting the severity level of the port scan (0135).

As per **claim 10, 22 and 35**, rejected as applied to claim 8, 21 and 34. Pruthi discloses: the reported severity varies as a function of the deviation from historical norm (0135-0138).

As per **claim 11, 23 and 37**, rejected as applied to claim 8, 21 and 34. Pruthi discloses: determining from the connection table statistics about TCP reset (RST) packets and ICMP port-unreachable packets to detect a spike in the number of RST packets and ICMP port-unreachable packets relative to the profile to increase the severity of a port scan event (0035, 0114, 0165, 0219).

As per **claim 12**, rejected as applied to claim 8. Pruthi discloses: determining occurs at the end of the first duration update periods to detect normal scans (0187-0188).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAOUSSEN BESROUR whose telephone number is (571)272-6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. B./
Examiner, Art Unit 2131
March 28, 2008
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131